PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-174796
(43)Date of publicati n f application : 23.06.2000

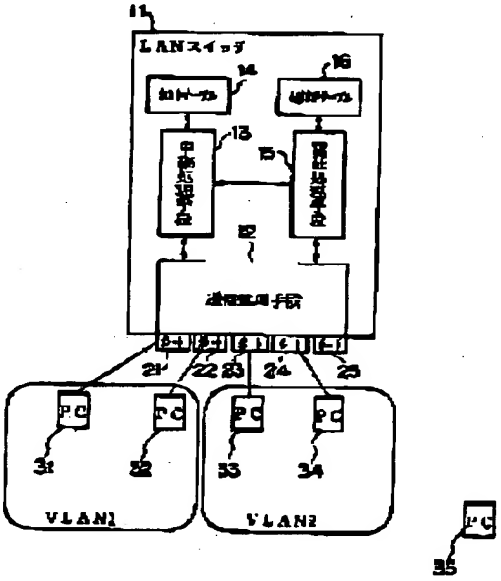
(51)Int.Cl. H04L 12/46
H04L 12/28
H04L 9/32
H04L 12/66
H04L 12/56
H04L 29/14

(21)Application number : 10-347235
(22)Date of filing : 07.12.1998

(71)Applicant : HITACHI LTD
(72)Inventor : TSUCHIYA KAZUAKI
NOZAKI SHINJI

(54) MANAGEMENT METHOD FOR COMMUNICATION NETWORK SYSTEM, AND INFORMATION REPEATER

(57)Abstract:
PROBLEM TO BE SOLVED: To facilitate the prevention of eavesdropping and impersonation by a malicious user and the analysis and restoration of an address setting error.
SOLUTION: An LAN switch 11 constitutes the communication network of a virtual LAN(VLAN) 1 and the VLAN 2, etc., by arbitrarily connecting plural personal computers(PCs) 31-34 as network terminals to respective plural ports 21-25. In this case, it is provided with a communication processing means 12 for transmitting and receiving packets with the respective ports 21-25, a relay processing means 13 for relaying the packets with the respective ports 21-25 based on a host table 14 updated by learning the change of the correspondence relation of the respective ports and the address information of the connected PC and an authentication processing means 15 for performing user authentication to the PC of a transmission origin by referring to an authentication table 16 and permitting the rewrite of the host table 14 and the relay of the packet only in the case of a true user at the time of the updating of the host table 14 of a packet relay trigger.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－174796
（Ｐ2000－174796Ａ）
(43)公開日　平成12年６月23日(2000.6.23)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/46		Ｈ０４Ｌ　11/00	３１０Ｃ	５Ｊ１０４
12/28		9/00	６７５Ａ	５Ｋ０３０
9/32		11/20	Ｂ	５Ｋ０３３
12/66			１０２Ｄ	５Ｋ０３５
12/56		13/00	３１１	９Ａ００１

審査請求　未請求　請求項の数３　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願平10－347235

(22)出願日　平成10年12月７日(1998.12.7)

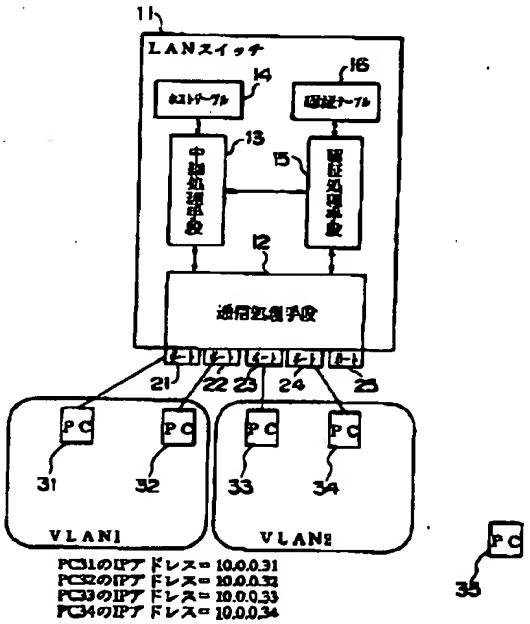
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　土屋　一暁
神奈川県海老名市下今泉810番地　株式会社日立製作所サーバ開発本部内
(72)発明者　野崎　信司
神奈川県海老名市下今泉810番地　株式会社日立製作所サーバ開発本部内
(74)代理人　100080001
弁理士　筒井　大和

最終頁に続く

(54)【発明の名称】　通信ネットワークシステムの管理方法および情報中継装置

(57)【要約】
【課題】　悪意のユーザによる盗聴やなりすましの防止、アドレス設定ミスの解析や回復を容易にする。
【解決手段】　複数のポート２１～２５の各々に任意にネットワーク端末としての複数のＰＣ３１～３４を接続することでＶＬＡＮ１およびＶＬＡＮ２等の通信ネットワークを構成するＬＡＮスイッチ１１において、各ポート２１～２５との間でパケットの送受信を行う通信処理手段１２と、各ポートと、接続されたＰＣのアドレス情報との対応関係の変化を学習して更新されるホストテーブル１４に基づき各ポート２１～２５間のパケットの中継を行う中継処理手段１３と、パケット中継装置のホストテーブル１４の更新時に、認証テーブル１６を参照して送信元のＰＣに対してユーザ認証を行い、真正のユーザの場合にのみホストテーブル１４の書き換えおよびパケットの中継を許可する認証処理手段１５とを備えた。

図　1



【特許請求の範囲】

【請求項１】　ネットワーク端末またはネットワーク中継装置が接続される複数の入出力ポートと、個々の前記入出力ポートと前記ネットワーク端末またはネットワーク中継装置に付与されたネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方を対応付けて格納する制御テーブルと、前記制御テーブルに基づいて複数の前記入出力ポートの各々に接続された前記ネットワーク端末またはネットワーク中継装置の相互間での通信情報の授受を行うとともに、前記通信情報に含まれる前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方と前記入出力ポートとの対応関係の変化を学習して前記制御テーブルを更新することで、前記入出力ポートに対する前記ネットワーク端末またはネットワーク中継装置の接続状態の動的な変更を可能にする中継処理手段とを含む情報中継装置を用いた通信ネットワークシステムの管理方法であって、

個々のネットワーク端末に対応した前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方と、当該ネットワーク端末のユーザ名およびパスワードとが対応付けて格納された認証テーブルを設定する第１のステップと、

前記制御テーブルの更新を伴う前記通信情報の授受が発生した時、前記通信情報の授受および前記制御テーブルの更新に先立って、前記通信情報の送信元および送信先の少なくとも一方のユーザに対して、前記ユーザ名およびパスワードの入力を要求し、入力されたユーザ名およびパスワードと前記認証テーブル内の前記ユーザ名およびパスワードとを照合するユーザ認証を実行し、前記ユーザ認証に成功したときのみ前記制御テーブルの更新および前記通信情報の授受を実行し、前記ユーザ認証に失敗したときは前記制御テーブルの更新を抑止するとともに前記通信情報を廃棄する第２のステップと、

を実行することを特徴とする通信ネットワークシステムの管理方法。

【請求項２】　請求項１記載の通信ネットワークシステムの管理方法において、

前記第１のステップでは、前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方に対して、前記ユーザおよび通信ネットワークシステムの管理者の少なくとも一方の連絡先メールアドレスも対応付けて設定し、前記第２のステップでは、前記ユーザ認証にて前記通信情報の送信元または送信先の前記ユーザから入力された前記ユーザ名を含むとともに前記制御テーブルの更新要求が発生したことを通知するメッセージを作成して該当する前記ネットワーク論理アドレスまたはネットワーク物理アドレスの前記ユーザおよび管理者の少なくとも一方の連絡先メールアドレスに対して送出する処理、

前記第２のステップでの前記ユーザ認証に失敗したとき、前記制御テーブルの更新を抑止するとともに前記通信情報を廃棄し、さらに当該通信情報を受信した前記入出力ポートの切り離し、および当該入出力ポートから受信した全ての通信情報を廃棄する処理、

前記第２のステップでの前記ユーザ認証に失敗したとき、前記制御テーブルの更新を抑止するとともに前記通信情報を廃棄し、さらに該通信情報の送信元の前記ネットワーク論理アドレスまたはネットワーク物理アドレスと同一の仮想ＬＡＮ（ローカル・エリア・ネットワーク）に属す全ての前記ネットワーク端末のユーザに、前記ネットワーク論理アドレスまたはネットワーク物理アドレス等の設定ミスや、悪意のユーザが他のネットワーク端末のアドレスを使って盗聴やなりすましの通信を行おうとしている可能性があることを警告するメッセージを作成して送る処理、

前記制御テーブルの更新要求発生の有無に関係なく、定期的または不定期に前記制御テーブル内に登録された前記ネットワーク論理アドレスまたはネットワーク物理アドレスのユーザに対して前記ユーザ認証を実行する処理、

の少なくとも一つの処理を実行することを特徴とする通信ネットワークシステムの管理方法。

【請求項３】　ネットワーク端末またはネットワーク中継装置が接続される複数の入出力ポートと、個々の前記入出力ポートと前記ネットワーク端末またはネットワーク中継装置に付与されたネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方を対応付けて格納する制御テーブルと、前記制御テーブルに基づいて複数の前記入出力ポートの各々に接続された前記ネットワーク端末またはネットワーク中継装置の相互間での通信情報の授受を行うとともに、前記通信情報に含まれる前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方と前記入出力ポートとの対応関係の変化を学習して前記制御テーブルを更新することで、前記入出力ポートに対する前記ネットワーク端末またはネットワーク中継装置の接続状態の動的な変更を可能にする中継処理手段とを含む情報中継装置であって、

個々のネットワーク端末に対応した前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方と、当該ネットワーク端末のユーザ名およびパスワードと、前記ユーザおよび通信ネットワークシステムの管理者の少なくとも一方の連絡先メールアドレスが対応付けて格納された認証テーブルと、

前記制御テーブルの更新を伴う前記通信情報の授受が発生した時、前記通信情報の授受および前記制御テーブルの更新に先立って、前記通信情報の送信元および送信先の少なくとも一方の前記ユーザに対して、ユーザ名およびパスワードの入力を要求し、入力されたユーザ名およびパスワードと前記認証テーブル内の前記ユーザ名およ

びパスワードと照合するユーザ認証を実行するとともに、前記通信情報の送信元および前記管理者の少なくとも一方の前記連絡先メールアドレスに対して前記ユーザ認証で得られた前記ユーザ名と前記制御テーブルの更新要求が発生したことを通知するメッセージを送信するとともに、前記ユーザ認証に成功したときのみ前記制御テーブルの更新および前記通信情報の授受を実行し、前記ユーザ認証に失敗したときは前記制御テーブルの更新を抑止するとともに前記通信情報を廃棄する動作を行う制御論理と、

を備えたことを特徴とする情報中継装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、通信ネットワークシステムの管理技術および情報中継技術に関し、特に、ＬＡＮ(LAN: Local Area Network) スイッチ(Layer2 スイッチ、Layer3スイッチ等）と呼ばれるインタネットワーク装置、およびＬＡＮスイッチで構成する通信ネットワークシステム（ＬＡＮスイッチネットワークシステム）の管理方法等に適用して有効な技術に関する。

【０００２】

【従来の技術】ＬＡＮスイッチが有する特徴技術にＶＬＡＮ(VLAN: Virtual LAN) がある。ＶＬＡＮはインタネットワーク装置の物理的なポートに依存せずにＬＡＮの構築を可能にする技術であり、その形式の違いによってポートベースＶＬＡＮ、ＭＡＣ(MAC: Media Access Control）アドレスベースＶＬＡＮ、Layer3プロトコルベースＶＬＡＮ、ＩＰ(IP: Internet Protocol）サブネットベースＶＬＡＮ等の名称で知られている。

【０００３】本発明の参考技術では、例えば図７に示すＩＰサブネットベースＶＬＡＮの通信ネットワークシステムにおいて複数のポート２２１～２２５を備えたＬＡＮスイッチ２１０はＰＣ(PC: Personal Computer）２３１からＰＣ２３３へのパケットを受信すると、パケットの始点ＭＡＣアドレス、終点ＭＡＣアドレス、始点ＩＰアドレスを学習してホストテーブル２２０を作成する。次に終点ＩＰアドレスをキーにホストテーブル２２０を参照し、該当エントリが有る場合は、該当ポートにパケットを出力する。該当エントリが無い場合は、ルーティングテーブル（図示無し）およびＡＲＰ(ARP: Address Resolution Protocol)テーブル（図示無し）を参照してネクストホップを決め、該当するホストテーブル２２０のエントリを新規に作成して、該当ポートにパケットを出力する。ＬＡＮスイッチ２１０はこのようにしてＰＣ２３１からＰＣ２３３へのパケットを中継する。

【０００４】さらにＬＡＮスイッチ２１０では、定期的にホストテーブル２２０のエントリを廃棄し、新たにパケットから学習することによって常にホストテーブル２２０のエントリを更新しているため、ＰＣが移動した場合でも移動先のポートにパケットを正しく中継することができる。すなわちＰＣは移動した場合でも移動前と同様の通信を自動的に再開することができる。

【０００５】

【発明が解決しようとする課題】しかしながら、上記参考技術には、次の技術的課題がある。

【０００６】第１の技術的課題は、ＩＰアドレス等の設定ミスに対して無防備なことである。例えばＰＣ２３２がＰＣ２３１のＩＰアドレスを誤って設定、ポート２２２に接続してしまったとする。この場合、ＬＡＮスイッチ２１０ではＰＣ２３１がポート２２１からポート２２２に移動したと判断し、そのようにホストテーブル２２０を書き換えてしまう。この結果、ＩＰアドレスを正しく使用しているＰＣ２３１が通信出来なくなる等の通信不良が発生する。また、ネットワークに接続されるＰＣの数が多い場合には、この通信不良の解析や回復には、多大の労力を要する。

【０００７】第２の技術的課題は、悪意のユーザによる盗聴やなりすましを許してしまうことである。例えばＰＣ２３５がＰＣ２３１のＩＰアドレスを設定、ポート２２５に接続したとする。この場合、ＬＡＮスイッチ２１０ではＰＣ２３１がポート２２１からポート２２５に移動したと判断し、そのようにホストテーブル２２０を書き換えてしまう。この結果、ＰＣ２３５がＰＣ２３１宛の通信データを受け取って盗聴したり、またＰＣ２３１になりすまして通信できてしまう。

【０００８】本発明の目的は、論理的あるいは物理的なネットワークアドレス等の設定ミスによる通信不良の防止や通信不良の原因解析および回復操作の迅速化が可能な通信ネットワークシステムの管理技術および情報中継技術を提供することにある。

【０００９】本発明の他の目的は、悪意のユーザによる盗聴やなりすましを防ぐことで通信ネットワークシステムのセキュリティを向上させることが可能な通信ネットワークシステムの管理技術および情報中継技術を提供することにある。

【００１０】

【課題を解決するための手段】本発明は、ＬＡＮスイッチ等の情報中継装置に備えられた複数の入出力ポートにユーザ端末や他の中継装置を接続して構築され、入出力ポートに対するユーザ端末等の接続状態の変化を学習して、入出力ポートとネットワークアドレスとの対応関係を管理する制御テーブルを更新することで、個々のユーザ端末の入出力ポートに対する接続状態を動的に変更することが可能な通信ネットワークの管理方法において、各ユーザ端末間、すなわち複数の入出力ポート間で通信情報の授受を契機とする制御テーブルの更新要求が発生した時、当該通信情報の送信元のユーザ端末に対してユーザ認証を実行し、真正のユーザであることが確認された場合にのみ、制御テーブルの更新およびそれに基づく通信情報の授受を行わせるものである。